

REMARKS

The following Request for Reconsideration is submitted in response to the Office Action issued on May 18, 2004 (Paper No. 8) in connection with the above-identified patent application, and is being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 106-181 remain pending in the present application, and stand rejected. Applicants respectfully request reconsideration and withdrawal of the rejection of such claims.

The Examiner has rejected claims 106-181 under 35 USC § 103(a) as being obvious over Downs et al. (U.S. Patent No. 6,574,609). Applicants respectfully traverse the § 103(a) rejection of claims 106-181.

Again, independent claim 106 recites a method in combination with a digital rights management (DRM) system operating on a computing device, where the DRM system employs a black box for performing decryption and encryption functions. The method is for obtaining the black box by the DRM system from a black box server. In the method, the DRM system requests the black box from the black box server and the black box server generates the black box, where such generated black box has a unique public / private key pair. The black box server then delivers the generated black box to the DRM system, and the DRM system installs the delivered black box therein.

Independent claim 122 recites subject matter similar to that in independent claim 106, but from the point of view of the DRM system. Independent claim 138 recites subject matter similar to that in independent claim 106, but from the point of view of the black box server. Independent claim 152 recites subject matter similar to that in independent claim 122, but in

the form of a computer-readable medium having computer-executable instructions thereon for performing the method of claim 122. Independent claim 168 recites subject matter similar to that in independent claim 138, but likewise in the form of a computer-readable medium having computer-executable instructions thereon for performing the method of claim 138.

Significantly, the black box as recited in the claims is not merely the unique public / private key pair, as the Examiner presumes, but instead is a device that performs encryption and decryption for the DRM system as part of such DRM system, and that employs the unique public / private key pair and other cryptographic keys to perform such encryption and decryption. As is set forth in the specification of the present application, the black box is trusted by the DRM system to perform the decryption and encryption functions for such DRM system, and also includes a version number and a unique signature, all as provided by an approved certifying authority.

The public key of the black box is made available to a license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key. The DRM system is initially provided with a black box with a public / private key pair, and the user is prompted to download from a black box server an updated secure black box when the user first requests a license. Such updated black box is written in unique executable code that will run only on the user's computing device, and is re-updated on a regular basis by downloading from the black box server. (Application, at page 4.)

The black box 30 works in conjunction with the license evaluator 36 to decrypt and encrypt certain information as part of the license evaluation function. In addition, once the license evaluator 36 determines that a user does in fact have the right to render the requested digital content 12 in the manner sought, the black box 30 is provided with a decryption key (KD) for such digital content 12, and performs the function of decrypting such digital content 12 based on such decryption key (KD). The license server 24 must trust that the black box 30 will perform the decryption function only in accordance with the license rules in the license 16, and also trust that such black box 30 will not operate should it become adulterated or otherwise modified by a user for the nefarious purpose of bypassing actual evaluation of a license 16. Accordingly, the black box 30 is also run in a protected or shrouded environment such that the user is denied access to such black box 30. (Application, pages 23-24.)

To summarize, then, Applicants respectfully submit that the Examiner should not and cannot merely characterize the recited black box of the claims as being with regard to encryption / decryption keys only. Instead, the recited black box is not merely a set of keys, but is a device that has a set of keys associated therewith and that performs cryptographic functions for the DRM system based at least in part on the associated set of keys. Applicants again respectfully submit that the failure of the Examiner to consider the claims of the present application in terms of the recited black box and not in terms of keys is *prima facie* improper.

Turning now to the Downs reference, it can be seen that such Downs reference discloses a system of managing protected content. The content is in the form of a secure container (SC) which includes the content encrypted by a symmetric key, the symmetric key encrypted by the recipient's public key, various digests, a digital certificate of the sender, and a signature. As seen in Fig. 1D, a recipient of the secure container employs a device 109 that

includes a decryption / re-encryption function 194 that is protected with tamper resistant code technology and that serves the purpose of decrypting and re-encrypting the content in a more amenable format and with a more amenable symmetric key. (Column 79, line 38 – column 80, line 14).

Significantly, although the Downs decryption / re-encryption function 194 acts in many respects as the black box of the present application, such Downs reference does not at all disclose or even recognize that such a decryption / re-encryption function 194 can become compromised over time and thus should be updated on a regular basis with a new a decryption / re-encryption function 194 from an appropriate server. In fact, the Downs reference does not disclose or even suggest any such server for updating the decryption / re-encryption function 194.

Thus, and more significantly, the Downs reference does not disclose or suggest that the Downs end-user device 109 should or could request an updated system decryption / re-encryption function 194 from an appropriate server, as is required by claims 106 et seq., or that such an appropriate server should or could generate same with a unique public / private key pair and deliver the generated function 194 to the device 109 such that the device 109 installs the delivered function 194 therein, as is also required by claims 106 et seq. Put simply, without appreciating that the function 194 should be updatable, the Downs reference simply fails to disclose or even suggest any mechanism by which such updating can take place.

Accordingly, Applicants respectfully submit that the Downs reference cannot be applied to make obvious independent claims 106, 122, 138, 152, and 168, or any claims

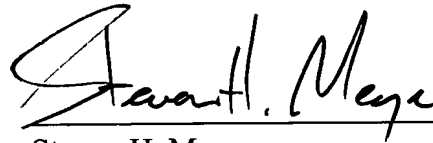
DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: May 18, 2004

PATENT

depending therefrom. Accordingly, Applicants respectfully request reconsideration and withdrawal of the § 103(a) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 106-181, is in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Steven H. Meyer", is written over a horizontal line.

Steven H. Meyer
Registration No. 37,189

Date: July 23, 2004

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439